Gold type codes of higher relative dimension

Chunlei Liu*†

Abstract

Let m, d, e, k be fixed positive integers such that

$$e = (m, d) = (m, 2d),\ 2 \leq k \leq \frac{m+e}{2e}.$$

Let s be a fixed maximum-length binary sequence of length $2^m - 1$. Let $(s_1, s_2, \cdots, s_{k-1})$ be a system of circular decimations of s whose decimation factors are respectively

$$2^d + 1, 2^{2d} + 1, \cdots, 2^{(k-1)d} + 1,$$

or respectively

$$2^d + 1, 2^{3d} + 1, \cdots, 2^{(2k-3)d} + 1,$$

or respectively

$$2^{(\frac{m-e}{2e})d} + 1, 2^{(\frac{m-3e}{2e})d} + 1, \cdots, 2^{(\frac{m+3e}{2e} - k)d} + 1.$$

Then $s_1, \cdots, s_{k-1}$ are maximum-length binary sequences of length $2^m - 1$. Let C be the $\mathbb{F}_2$-vector space generated by all circular shifts of $s, s_1, \cdots, s_{k-1}$. Then C has an $\mathbb{F}_{2^m}$-vector space structure, and is of dimension k over $\mathbb{F}_{2^m}$. When $k = 2$, C is the Gold code. So we regard C as a Gold type code of relative dimension k. The DC component distribution of C is explicitly calculated out in the present paper.

Key phrases: Gold code, cyclic code, alternating form
MSC: 94B15, 11T71.

1 INTRODUCTION

Let q be a prime power, and C an $[n, k]$-linear code over $\mathbb{F}_q$. The weight of a codeword $c = (c_0, c_1, \cdots, c_{n-1})$ of C is defined to be

$$\mathrm{wt}(c) = \#\{0 \leq i \leq n-1 \mid c_i \neq 0\}.$$

For each $i = 0, 1, \cdots, n$, define

$$A_i = \#\{c \in C \mid \ \mathrm{wt}(c) = i\}.$$

*Dept. of math., Shanghai Jiao Tong Univ., Sahnghai 200240, China, clliu@sjtu.edu.cn.
†Dengbi Technologies Cooperation Limited., Yichun 336099, China, 714232747@qq.com.

The sequence $(A_0, A_1, \cdots, A_n)$ is called the weight distribution of C. Given a linear code C, it is challenging to determine its weight distribution. The weight distribution of Gold codes was determined by Gold [G66–G68]. The weight distribution of Kasami codes was determined by Kasami [K66]. The weight enumerators of Gold type and Kasami type codes of higher relative dimension were determined by Berlekamp [Ber] and Kasami [K71]. The weight distribution of the p-ary analogue of Gold codes was determined by Trachtenberg [Tr]. The weight distribution of the circular decimation of the p-ary analogue of Gold codes with decimation factor 2 was determined by Feng-Luo [FL]. The weight distribution of the p-ary analogue of Gold type codes of relative dimension 3 was determined by Zhou-Ding-Luo-Zhang [ZDLZ]. The weight distribution of the circular decimation with decimation factor 2 of the p-ary analogue of Gold type codes of relative dimension 3 was determined by Zheng-Wang-Hu-Zeng [ZWHZ]. The weight distribution of (the p-ary analogue of) Kasami type codes of maximum relative dimension was determined by Li-Hu-Feng-Ge [LHFG]. The weight distribution of the p-ary analogue of Gold type codes of higher relative dimension was determined by Schmidt [Sch]. The weight distribution of some other classes of cyclic codes was determined in the papers [AL], [BEW], [BMC], [BMC10], [BMY], [De], [DLMZ], [DY], [FE], [FM], [KL], [LF], [LHFG], [LN], [LYL], [LTW], [MCE], [MCG], [MO], [MR], [MY], [MZLF], [RP], [SC], [VE], [WTQYX], [XI], [XI12], [YCD], [YXDL] and [ZHJYC].

Let m, d, e, k be fixed positive integers such that

$$e = (m, d) = (m, 2d), \ 2 \leq k \leq \frac{m+e}{2e}.$$

Let s be a fixed maximum-length binary sequence of length $2^m - 1$. Let $(s_1, s_2, \cdots, s_{k-1})$ be a system of circular decimations of s whose decimation factors are respectively

$$2^d + 1, 2^{2d} + 1, \cdots, 2^{(k-1)d} + 1,$$

or respectively

$$2^d + 1, 2^{3d} + 1, \cdots, 2^{(2k-3)d} + 1,$$

or respectively

$$2^{(\frac{m-e}{2e})d} + 1, 2^{(\frac{m-3e}{2e})d} + 1, \cdots, 2^{(\frac{m+3e}{2e} - k)d} + 1.$$

Then $s_1, \cdots, s_{k-1}$ are maximum-length binary sequences of length $2^m - 1$. Let C be the $\mathbb{F}_2$-vector space generated by all circular shifts of $s, s_1, \cdots, s_{k-1}$. If $d = e = 1$, then C is the code studied by Berlekamp [Ber] and Kasami [K71]. Let $\{Q_{\vec{a}}\}$ be the system

$$Q_{\vec{a}}(x) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_0 x) + \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j x^{2^{jd}+1}), \ \vec{a} \in \mathbb{F}_{2^m}^k,$$

or the system

$$Q_{\vec{a}}(x) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_0 x) + \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j x^{2^{(2j-1)d}+1}), \ \vec{a} \in \mathbb{F}_{2^m}^k,$$

or the system

$$Q_{\vec{a}}(x) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_0x) + \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j x^{2^{(\frac{m+e}{2e}-j)d}+1}),\ \vec{a} \in \mathbb{F}_{2^m}^k.$$

Then

$$C = \{c_{\vec{a}} \mid \ \vec{a} \in \mathbb{F}_{2^m}^k\},$$

where $c_{\vec{a}} = (\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(\pi^{-i}))_{i=0}^{2^m-2}$ with π being a primitive element of $\mathbb{F}_{2^m}$. The correspondence $\vec{a} \mapsto c_{\vec{a}}$ defines an $\mathbb{F}_{2^m}$-vector space structure on C, and C is of dimension k over $\mathbb{F}_{2^m}$. When $k=2$, C is the Gold code. So we call C a Gold type code of relative dimension k.

One can prove the following.

Theorem 1.1 *If $c \in C$ is nonzero, then*

$$\mathrm{DC}(c) \in \{-1, -1 \pm 2^{\frac{m+e}{2}+je} \mid \ j = 0,1,2,\cdots,k-2\},$$

where

$$\mathrm{DC}(c) = 2^m - 1 - 2\mathrm{wt}(c) = \sum_{i=0}^{2^m-2} (-1)^{c_i}$$

is the DC component of $c = (c_0, c_1, \cdots, c_{2^m-2}) \in C$.

The present paper is concerned with the frequencies

$$\alpha_{r,\varepsilon} = \#\{0 \neq c \in C \mid \ \mathrm{DC}(c) = -1 + \varepsilon 2^{m-\frac{er}{2}}\},\ r = 0,2,4,\cdots,\frac{m-e}{e}. \qquad (1)$$

The main result of the present paper is the following.

Theorem 1.2 *For each $j = 0,1,\cdots,k-2$, and for each $\varepsilon = \pm 1$, we have*

$$\alpha_{\frac{m-e}{e}-2i,\varepsilon} = \frac{1}{2}(2^{m-e-2ei} + \varepsilon 2^{\frac{m-e}{2}-ei}) \sum_{j=i}^{k-2} (-1)^{j-i} 4^{e\binom{j-i}{2}} \binom{j}{i}_{4^e} \binom{\frac{m-e}{2e}}{j}_{4^e} (2^{m(k-1-j)}-1),$$

where $\binom{j}{i}_q$ is a Gaussian binomial coefficient.

From the above theorem one can deduce the following.

Theorem 1.3 *We have*

$$\begin{aligned} &\#\{c \in C \mid \ \mathrm{DC}(c) = -1\} \\ &= 2^{mk} - 1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2} (2^{m(k-u)} - 2^m) \prod_{j=0}^{u-1} (2^m - 2^{e(2j+1)}) \\ &\approx 2^{mk}(1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2}). \end{aligned}$$

If $d = e = 1$, then the weight enumerator of C is determined by Berlekamp [Ber] and Kasami [K71]. However, some extra calculations are needed to explicitly write out the coefficients of the weight enumerators in [Ber, K71].

2 ENTERING BILINEAR FORMS I

In this section we shall prove Theorem 1.1.

Note that

$$1 + \mathrm{DC}(c_{\vec{a}}) = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}. \tag{2}$$

It is well-known that

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))} = \begin{cases} 0, & 2\nmid \mathrm{rk}(Q_{\vec{a}}), \\ \pm 2^{m-e\cdot\frac{\mathrm{rk}(Q_{\vec{a}})}{2})}, & 2|\mathrm{rk}(Q_{\vec{a}}). \end{cases} \tag{3}$$

Let

$$B_{\vec{a}}(x,y) = Q_{\vec{a}}(x+y) - Q_{\vec{a}}(x) - Q_{\vec{a}}(y).$$

Then $\{B_{\vec{a}}\}$ is either the system

$$B_{\vec{a}}(x,y) = \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j(xy^{2^{jd}} + x^{2^{jd}}y)),\ \vec{a}\in\mathbb{F}_{2^m}^k, \tag{4}$$

or the system

$$B_{\vec{a}}(x,y) = \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j(xy^{2^{(2j-1)d}} + x^{2^{(2j-1)d}}y)),\ \vec{a}\in\mathbb{F}_{2^m}^k, \tag{5}$$

or the system

$$B_{\vec{a}}(x,y) = \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j(xy^{2^{(\frac{m+e}{2e}-j)d}} + x^{2^{(\frac{m+e}{2e}-j)d}}y)),\ \vec{a}\in\mathbb{F}_{2^m}^k. \tag{6}$$

It is well-known that

$$\mathrm{rk}(B_{\vec{a}}) = \begin{cases} \mathrm{rk}(Q_{\vec{a}}), & 2\mid \mathrm{rk}(Q_{\vec{a}}), \\ \mathrm{rk}(Q_{\vec{a}})-1, & 2\nmid \mathrm{rk}(Q_{\vec{a}}). \end{cases} \tag{7}$$

We now prove Theorem 1.1. By (2), (3) and (7), it suffices to prove the following.

Theorem 2.1 *If* $(a_1,\cdots,a_{k-1})\neq 0$, *then*

$$\mathrm{rk}(B_{\vec{a}}) \geq \frac{m-e}{e} - 2(k-2).$$

Proof. Suppose that $(a_1,\cdots,a_{k-1})\neq 0$. It suffices to show that

$$\dim_{\mathbb{F}_{2^e}} \mathrm{Rad}(B_{\vec{a}}) \leq 2(k-1),$$

where

$$\mathrm{Rad}(B_{\vec{a}}) = \{x\in\mathbb{F}_{2^m} \mid\ B_{\vec{a}}(x,y)=0,\ \forall y\in\mathbb{F}_{2^m}\}.$$

Without loss of generality, we assume that $\{B_{\vec{a}}\}$ is the system (4). Then

$$\begin{aligned}\mathrm{Rad}(B_{\vec{a}}) &= \{x \in \mathbb{F}_{2^m} | \sum_{j=1}^{k-1} (a_j^{2^{-jd}} x^{2^{-jd}} + a_j x^{2^{jd}}) = 0\} \\ &= \{x \in \mathbb{F}_{2^m} | \sum_{j=1}^{k-1} (a_j^{2^{(k-1-j)d}} x^{2^{(k-1-j)d}} + a_j^{2^{(k-1)d}} x^{2^{(k-1+j)d}}) = 0\}.\end{aligned}$$

Note that

$$\{x \in \mathbb{F}_{2^{md/e}} | \sum_{j=1}^{k-1} (a_j^{2^{(k-1-j)d}} x^{2^{(k-1-j)d}} + a_j^{2^{(k-1)d}} x^{2^{(k-1+j)d}}) = 0\}.$$

is a subspace of $\mathbb{F}_{2^{md/e}}$ over $\mathbb{F}_{2^d}$ of dimension $\leq 2(k-1)$. As $(m,d)=e$, a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^e}$ is also a basis of $\mathbb{F}_{2^{md/e}}$ over $\mathbb{F}_{2^d}$. It follows that

$$\dim_{\mathbb{F}_{2^e}} \mathrm{Rad}(B_{\vec{a}}) \leq 2(k-1).$$

The theorem is proved. ■

3 ENTERING BILINEAR EQUATIONS II

In this section we shall reduce Theorem 1.2 to the following.

Theorem 3.1 *We have, for $0 \leq i \leq k-2$,*

$$\beta_{\frac{m-e}{e}-2i} = \sum_{j=i}^{k-2} (-1)^{j-i} 2^{e(j-i)(j-i-1)} \binom{j}{i}_{4^e} \binom{\frac{m-e}{2e}}{j}_{4^e} (2^{m(k-1-j)}-1),$$

where

$$\beta_r = 2^{-m} \#\{\vec{a} \in \mathbb{F}_{2^m}^k \mid \ \mathrm{rk}(B_{\vec{a}}) = r,\ (a_1, \cdots, a_{k-1}) \neq 0\}. \qquad (8)$$

It suffices to prove the following.

Theorem 3.2 *For each $r = 0, 2, \cdots, \frac{m-e}{e}$,*

$$\alpha_{r,\varepsilon} = \frac{1}{2}(2^{er} + \varepsilon 2^{\frac{er}{2}})\beta_r,$$

Proof. By (1), (2), (3), (7), and (8),

$$\begin{aligned}& 2^{m-\frac{er}{2}}(\alpha_{r,1} - \alpha_{r,-1}) \\ &= \sum_{\mathrm{rk}(B_{\vec{a}})=r} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))} \\ &= 2^{-m} \sum_{c \in \mathbb{F}_{2^m}} \sum_{\mathrm{rk}(B_{\vec{a}})=r} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(cx) + Q_{\vec{a}}(x))} \\ &= 2^{-m} \sum_{\mathrm{rk}(B_{\vec{a}})=r} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))} \sum_{c \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(cx)} \\ &= 2^m \beta_r.\end{aligned}$$

Similarly,

$$
\begin{aligned}
&2^{2m-er}(\alpha_{r,1}+\alpha_{r,-1}) \\
&= \sum_{\mathrm{rk}(B_{\vec{a}})=r} \Big(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}\Big)^2 \\
&= 2^{-m} \sum_{c\in\mathbb{F}_{2^m}} \sum_{\mathrm{rk}(B_{\vec{a}})=r} \Big(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(cx)+Q_{\vec{a}}(x))}\Big)^2 \\
&= 2^{-m} \sum_{\mathrm{rk}(B_{\vec{a}})=r} \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x)+Q_{\vec{a}}(y))} \sum_{c\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(c(x+y))} \\
&= 2^{2m}\beta_r.
\end{aligned}
$$

The theorem is proved.■

4 ASSOCIATION SCHEME THEORETIC APPROACH

In this section we shall use the following theorem of Delarte-Goethals to prove Theorem 3.1.

Theorem 4.1 ([DG]) *Let M be an odd number, X the space of alternating bilinear forms on an M-dimension vector space over $\mathbb{F}_q$, Y a subspace of X, and*

$$d(Y) = \min\{\mathrm{rk}(y) \mid 0 \neq y \in Y\}.$$

Then

$$|Y| \leq q^{M(M-d(Y)+1)/2}.$$

Moreover, if the equality holds, then, for $i \leq (M-1-d(Y))/2$,

$$
\begin{aligned}
&\#\{y \in Y \mid \ \mathrm{rk}(y) = M-1-2i\} \\
&= \sum_{j=i}^{(M-1-d(Y))/2} (-1)^{j-i} q^{(j-i)(j-i-1)} \binom{j}{i}_{q^2} \binom{(M-1)/2}{j}_{q^2} (q^{M(M-d(Y)+1-2j)/2}-1).
\end{aligned}
$$

We now the above theorem to prove Theorem 3.1.

Let X be the space of alternating $\mathbb{F}_{2^e}$-bilinear forms on $\mathbb{F}_{2^m}$. Fix a system $\{B_{\vec{a}}\}$. Set

$$Y = \{B_{\vec{a}} \mid \ \vec{a} \in \mathbb{F}_{2^m}^k, a_0 = 0\}.$$

By Theorem 2.1,

$$d(Y) \geq \frac{m-e}{e} - 2(k-2).$$

By Delsarte-Goethals' theorem,

$$|Y| \leq 2^{m(\frac{m+e}{e}-d(Y))/2} \leq 2^{m(k-1)}.$$

As $|Y| = 2^{m(k-1)}$, we arrive at

$$|Y| = 2^{m(\frac{m+e}{e}-d(Y))/2} = 2^{m(k-1)}.$$

In particular, $d(Y) = \frac{m-e}{e} - 2(k-2)$. Applying Delsarte-Goethals' theorem one more time, we have, for $0 \le i \le k-2$,

$$\begin{aligned}
&\#\{\vec{a} \in \mathbb{F}_{2^m}^k \mid \operatorname{rk}(B_{\vec{a}}) = \frac{m-e}{e} - 2i, a_0 = 0\} \\
&= \sum_{j=i}^{k-2} (-1)^{j-i} 2^{e(j-i)(j-i-1)} \binom{j}{i}_{4^e} \binom{\frac{m-e}{2e}}{j}_{4^e} (2^{m(k-1-j)} - 1).
\end{aligned}$$

Theorem 3.1 is proved.

5 NUMBER THEORETIC APPROACH

The theorem of Delarte-Goethals we used in the last section is proved by developing the theory of association schemes. To make the present paper self-contained, we shall develop a number theoretic approach, which is similar to the approach of Berlekamp [Ber] and Kasami [K71].

Let $V_{s,u}$ be the set of solutions $(x_1, x_2, \cdots, x_{2u}) \in \mathbb{F}_{2^m}^{2u}$ of one of the systems

$$\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2^{jd}} + x_{2i-1}^{2^{jd}} x_{2i}) = 0, \ j = 1, 2, \cdots, s, \tag{9}$$

$$\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2^{(2j-1)d}} + x_{2i-1}^{2^{(2j-1)d}} x_{2i}) = 0, \ j = 1, 2, \cdots, s, \tag{10}$$

and

$$\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2^{(\frac{m+e}{2e} - j)d}} + x_{2i-1}^{2^{(\frac{m+e}{2e} - j)d}} x_{2i}) = 0, \ j = 1, 2, \cdots, s. \tag{11}$$

In this section we shall use the following theorem to prove Theorem 3.1.

Theorem 5.1 *If $s \ge u \ge 1$, then $V_{s,u} = V_{u,u}$.*

We now prove Theorem 3.1. We shall make repeated use of the following q-binomial formula

$$\prod_{i=0}^{u-1} (1 + q^i t) = \sum_{i=0}^{u} q^{\binom{i}{2}} \binom{u}{i}_q t^i.$$

By the orthogonality of characters and Theorem 5.1, we have

$$\sum_{\vec{a} \in \mathbb{F}_{2^m}^k} \Big(\sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{\operatorname{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(B_{\vec{a}}(x,y))} \Big)^u = 2^{mk} |V_{u,u}|, \ 0 \le u \le k-1,$$

where $|V_{0,0}| = 1$. Applying the identity

$$\sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{\operatorname{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(B_{\vec{a}}(x,y))} = 2^{2m - e \cdot \operatorname{rk}(B_{\vec{a}})},$$

we arrive at

$$\sum_{2 | r = \frac{m-e}{e} - 2(k-2)}^{\frac{m-e}{e}} \beta_r 2^{u(2m-er)} = 2^{m(k-1)} |V_{u,u}| - 2^{2mu}, \ 0 \le u \le k-1.$$

That is,

$$\sum_{i=0}^{k-2}\beta_{\frac{m-e}{e}-2i}4^{eui}=2^{m(k-1)-(m+e)u}|V_{u,u}|-2^{(m-e)u},\ 0\le u\le k-1.$$

Consider the equation

$$\sum_{i=0}^{k-2}\beta_{\frac{m-e}{e}-2i}\begin{pmatrix}1\\4^{ei}\\\vdots\\4^{e(k-1)i}\end{pmatrix}=\begin{pmatrix}2^{m(k-1)}|V_{0,0}|-1\\2^{m(k-1)-(m+e)}|V_{1,1}|-2^{m-e}\\\vdots\\2^{-(k-1)e}|V_{k-1,k-1}|-2^{u(m-e)}\end{pmatrix}$$

Multiplying on the left by the row vector $((-1)^{k-1-i}4^{e\binom{k-1-i}{2}}\binom{k-1}{i}_{4^e})_{i=0}^{k-1}$, and applying the q-binomial formula, we arrive at

$$\sum_{i=0}^{k-1}(-1)^{k-1-i}4^{e\binom{k-1-i}{2}}\binom{k-1}{i}_{4^e}(2^{m(k-1)-(m+e)i}|V_{i,i}|-2^{(m-e)i})=0.$$

Applying the q-binomial formula once more, we arrive at

$$\sum_{i=0}^{k-1}(-1)^{k-1-i}4^{e\binom{k-1-i}{2}}\binom{k-1}{i}_{4^e}2^{m(k-1)-(m+e)i}|V_{i,i}|=\prod_{i=0}^{k-1}(2^{(m-e)i}-4^{ei}).$$

Replacing $k-1$ with an arbitrary positive integer u, we arrive at

$$\sum_{i=0}^{u}(-1)^{u-i}4^{e\binom{u-i}{2}}\binom{u}{i}_{4^e}2^{mu-(m+e)i}|V_{i,i}|=\prod_{i=0}^{k-1}(2^{(m-e)i}-4^{ei}).$$

That is,

$$\sum_{i=0}^{u}(-1)^{u-i}4^{e\binom{u-i}{2}}\binom{u}{i}_{4^e}2^{-(m+e)i}|V_{i,i}|=2^{-mu}\prod_{i=0}^{k-1}(2^{(m-e)i}-4^{ei}).\tag{12}$$

Now fix $0\le u\le k-1$, and consider the equation

$$\sum_{i=0}^{k-2}\beta_{\frac{m-e}{e}-2i}\begin{pmatrix}1\\4^{ei}\\\vdots\\4^{eui}\end{pmatrix}=\begin{pmatrix}2^{m(k-1)}|V_{0,0}|-1\\2^{m(k-1)-(m+e)}|V_{1,1}|-2^{m-e}\\\vdots\\2^{-(k-1)e}|V_{u,u}|-2^{u(m-e)}\end{pmatrix}$$

Multiplying on the left by the row vector $((-1)^{u-i}q^{\binom{u-i}{2}}\binom{u}{i}_q)_{i=0}^{u}$, and applying the q-binomial formula as well as (12), we arrive at

$$\sum_{i=u}^{k-2}\beta_{\frac{m-e}{e}-2i}\prod_{0\le h\le u-1}(4^{ei}-4^{eh})=(2^{m(k-1-u)}-1)\prod_{0\le h\le u-1}(2^{m-e}-4^{eh}).$$

Dividing both sides by $\prod_{0\le h\le u-1}(4^{eu}-4^{eh})$, we arrive at

$$\sum_{i=u}^{k-2}\beta_{\frac{m-e}{e}-2i}\binom{i}{u}_{4^e}=\binom{\frac{m-e}{2e}}{u}_{4^e}(2^{m(k-1-u)}-1).$$

Applying the q-binomial Möbius inversion formula

$$\sum_{i=v}^{u}(-1)^{i-v}q^{\binom{i-v}{2}}\binom{i}{v}_q\binom{u}{i}_q=\begin{cases}1, & u=v,\\ 0, & u\neq v,\end{cases}$$

we arrive at

$$\beta_{\frac{m-e}{e}-2j}=\sum_{u=j}^{k-2}(-1)^{u-j}4^{e\binom{u-j}{2}}\binom{\frac{m-e}{2e}}{u}_{4^e}\binom{u}{j}_{4^e}(2^{m(k-1-u)}-1).$$

Theorem 3.1 is proved.

6 SYSTEMS OF BILINEAR EQUATIONS

In this section we shall prove Theorem 5.1. We begin with the following.

Theorem 6.1 *The systems (9), (10), and (11) are respectively equivalent to the systems*

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^d}+x_{2i-1}^{2^d}x_{2i})=0,\\ \sum_{i=1}^{u}(\tilde{x}_{2i-1}\tilde{x}_{2i}^{2^{jd}}+\tilde{x}_{2i-1}^{2^{jd}}\tilde{x}_{2i})=0,\\ j=1,2,\cdots,s-1,\end{cases}\tag{13}$$

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^d}+x_{2i-1}^{2^d}x_{2i})=0,\\ \sum_{i=1}^{u}(\tilde{x}_{2i-1}\tilde{x}_{2i}^{2^{(2j-1)d}}+\tilde{x}_{2i-1}^{2^{(2j-1)d}}\tilde{x}_{2i})=0,\\ j=1,2,\cdots,s-1,\end{cases}\tag{14}$$

and

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{m-e}{2e})d}}+x_{2i-1}^{2^{(\frac{m-e}{2e})d}}x_{2i})=0,\\ \sum_{i=1}^{u}(\tilde{x}_{2i-1}\tilde{x}_{2i}^{2^{(\frac{m+e}{2e}-j)d}}+\tilde{x}_{2i-1}^{2^{(\frac{m+e}{2e}-j)d}}\tilde{x}_{2i})=0,\\ j=1,2,\cdots,s-1,\end{cases}\tag{15}$$

where $\tilde{x}_i=x_i+x_i^{2^d},\ x_i+x_i^{2^{2d}}$, *and* $x_i+x_i^{2^{-d}}$ *respectively.*

Proof. We deal with the system (9) first. Adding 2^d-th power of the $(j-1)$-th equation to the j-th equation, we arrive at

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^d}+x_{2i-1}^{2^d}x_{2i})=0,\\ \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{jd}}+x_{2i-1}^{2^{jd}}x_{2i}+x_{2i-1}^{2^d}x_{2i}^{2^{jd}}+x_{2i-1}^{2^{jd}}x_{2i}^{2^d})=0,\\ j=2,3,\cdots,s.\end{cases}$$

Adding the $(j-1)$-th equation to the j-th equation in the above system, we arrive at the system (13).

We now deal with the system (10). Adding 2^{2d}-th power of the $(j-1)$-th equation to the j-th equation, we arrive at

$$\begin{cases} \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^d}+x_{2i-1}^{2^d}x_{2i})=0, \\ \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(2j-1)d}}+x_{2i-1}^{2^{(2j-1)d}}x_{2i}+x_{2i-1}^{2^d}x_{2i}^{2^{(2j-1)d}}+x_{2i-1}^{2^{(2j-1)d}}x_{2i}^{2^d})=0, \\ j=2,3,\cdots,s. \end{cases}$$

Adding the $(j-1)$-th equation to the j-th equation in the above system, we arrive at the system (14).

Finally we deal with the system (11). Inserting $2^{\frac{m+e}{2e}}$-th power of the first equation to the system, we arrive at the system

$$\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{m+e}{2e}-j)d}}+x_{2i-1}^{2^{(\frac{m+e}{2e}-j)d}}x_{2i})=0,\ j=0,1,2,\cdots,s.$$

Adding the 2^{-d}-th power of the $(j-1)$-th equation to the j-th equation in the above system, we arrive at

$$\begin{cases} \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{m-e}{2e})d}}+x_{2i-1}^{2^{(\frac{m-e}{2e})d}}x_{2i})=0, \\ \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{m+e}{2e}-j)d}}+x_{2i-1}^{2^{(\frac{m+e}{2e}-j)d}}x_{2i}+x_{2i-1}^{2^{-d}}x_{2i}^{2^{(\frac{m+e}{2e}-j)d}}+x_{2i-1}^{2^{(\frac{m+e}{2e}-j)d}}x_{2i}^{2^{-d}})=0, \\ j=1,2,\cdots,s. \end{cases}$$

Adding the $(j-1)$-th equation to the j-th equation in the above system, we arrive at the system (15). Theorem 6.1 is proved. ■

We now prove Theorem 5.1. If $u=1$, then $V_{s,u}=V_{u,u}$ trivially. Now assume that $u\geq 2$. Suppose that $(x_1,x_2,\cdots,x_{2u})$ belongs to $V_{u,u}$. We are going to show that $(x_1,x_2,\cdots,x_{2u})$ belongs to $V_{s,u}$. By induction, we may assume that $x_{2u}\neq 0$. Then we may further assume that $x_{2u}=1$. By Theorem 6.1, $(\tilde{x}_1,\tilde{x}_2,\cdots,\tilde{x}_{2u})\in V_{u-1,u}$. As $\tilde{x}_{2u}=0$, we see that $(\tilde{x}_1,\tilde{x}_2,\cdots,\tilde{x}_{2u-2})\in V_{u-1,u-1}$. By induction, $(\tilde{x}_1,\tilde{x}_2,\cdots,\tilde{x}_{2u-2})\in V_{s-1,u-1}$. As $\tilde{x}_{2u}=0$, we see that $(\tilde{x}_1,\tilde{x}_2,\cdots,\tilde{x}_{2u})\in V_{s-1,u}$. By Theorem 6.1, $(x_1,x_2,\cdots,x_{2u})$ belongs to $V_{s,u}$. Theorem 5.1 is proved.

7 THE NUMBER OF BALANCED SEQUENCES

In this section we prove Theorem 1.3. We have

$$\begin{aligned}
&\#\{c \in C \mid \mathrm{DC}(c) = -1\} \\
=&2^{mk} - 1 - \sum_{j=0}^{\frac{m-e}{2e}} 2^{m-e-2ej} \sum_{u=j}^{k-2} (-1)^{u-j} 4^{e\binom{u-j}{2}} \binom{\frac{m-e}{2e}}{u}_{4^e} \binom{u}{j}_{4^e} (2^{m(k-1-u)} - 1) \\
=&2^{mk} - 1 - 2^{m-e} \sum_{u=0}^{k-2} 4^{-eu} \binom{\frac{m-e}{2e}}{u}_{4^e} (2^{m(k-1-u)} - 1) \sum_{j=0}^{u} (-1)^j 4^{ej} 4^{e\binom{j}{2}} \binom{u}{j}_{4^e} \\
=&2^{mk} - 1 - 2^{m-e} \sum_{u=0}^{k-2} 4^{-eu} \binom{\frac{m-e}{2e}}{u}_{4^e} (2^{m(k-1-u)} - 1) \prod_{j=1}^{u} (1 - 4^{ej}) \\
=&2^{mk} - 1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2} (2^{m(k-u)} - 2^m) \prod_{j=0}^{u-1} (2^m - 2^{e(2j+1)}) \\
&\approx 2^{mk} (1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2}).
\end{aligned}$$

Theorem 1.3 is proved.

Acknowledgement. The author thanks Kai-Uwe Schmidt for telling him the background of this subject.

References

[AL] Y. Aubry, P. Langevin, On the weights of binary irreducible cyclic codes, in Proc. Int. Conf. Cod. Cryptography, 2006, pp. 46-54.

[BMC] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, Inf. Control, vol. 20, no. 2, pp. 158-175, 1972.

[BMY] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progress Rep., vol. 16, pp. 128-131, 1973.

[Ber] E. R. Berlekamp, The weight enumerators for certain subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 17: 485-500, 1970.

[BEW] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi Sums. New York, NY, USA: Wiley, 1997.

[BMC10] N. Boston, G. McGuire, The weight distributions of cyclic codes with two zeros and zeta functions, J. Symbol. Comput., vol. 45, no. 7, pp. 723-733, 2010.

[De] P. Delsarte, On subfield subcodes of modified reed-solomon codes, IEEE Trans. Inf. Theory, vol. 21, no. 5, pp. 575-576, 1975.

[DG] P. Delsarte, J.-M. Goethals, Alternating blinear forms over GF(q), J. Comb. Theory (A) 19 (1): 26-50, 1975.

[DLMZ] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory, vol. 57, no. 12, pp. 8000-8006, 2011.

[DY] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discr. Math., vol. 313, pp. 434-446, 2013.

[FL] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes,Finite Fields Appl., vol. 14, no. 2, pp. 390-409, 2008.

[FE] T. Feng, On cyclic codes of length 2^{2^r} with two zeros whose dual codes have three weights, Des. Codes Cryptogr., vol. 62, pp. 253-258, 2012.

[FM] T. Feng K. Momihara, Evaluation of the weight distribution of a class of cyclic codes based on Index 2 Gauss sums, 2012, preprint.

[G66] R. Gold, Characteristic linear sequences and their coset functions, J. SIAM Appl. Math. 14 (5): 980-985, 1966.

[G67] R. Gold, Optimal binary sequences for spread spectrum multiplexing, IEEE Trans. Inform. Theory 13 (4): 619-621, 1967.

[G68] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inform. Theory 14 (1): 154-156, 1968.

[K66] T. Kasami, Weight distribution formula for some cyclic codes, Univ. of Illinois, Rept. R-265, 1966.

[K71] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 18: 369-394, 1971.

[KL] T. Kløve, Codes for Error Detection. Hackensack, NJ, USA: World Scientific, 2007.

[LHFG] S. X. Li, S. H. Hu, T. Feng and G. Ge, The weight distribution of a class of cyclic codes related to Hermitian graphs, IEEE Trans. Inf. Theory, vol. 59, no. 5, pp. 3064-3067, 2013.

[LN] R. Lidl H. Nuederreuter, Finite Fields. NewYork, NY, USA: Addision-Wesley, 1983.

[LYL] Y. Liu, H. Yan and C. Liu, A class of six-weight cyclic codes and their weight distribution, Des. Codes Cryptogr., to appear.

[LF] J. Luo K. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5332-5344, Dec. 2008.

[LTW] J. Luo, Y. Tang, H. Wang, Cyclic codes and sequences: the generalized Kasami case, IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2130-2142, May 2010.

[MZLF] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 397-402, Jan. 2011.

[MCE] R. J. McEliece, Irreducible cyclic codes and Gauss sums, in Part 1: Theory of Designs, Finite Geometry and Coding Theory, Math. Centre Tracts, Math. Centrum, ser. Combinatorics: NATO Advanced Study Institute Series. Amsterdam, The Netherlands: Springer, 1974, pp. 179-196.

[MCG] G. McGuire, On three weights in cyclic codes with two zeros, Finite Fields Appl., vol. 10, no. 1, pp. 97-104, 2004.

[MO] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inf. Theory, vol. 53, no. 2, pp. 843-847, Feb. 2007.

[MR] M. Moisio, K. Ranto, Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros, Finite Fields Appl., vol. 13, no. 4, pp. 922-935, 2007.

[MY] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., vol. 39, pp. 251-264, 1981.

[RP] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 2568-2570, Jun. 2010.

[SC] R. Schoof, Families of curves and weight distribution of codes, Bull. Amer. Math. Soc., vol. 32, no. 2, pp. 171-183, 1995.

[Sch] K. Schmidt, Symmetric bilinear forms over finite fields with applications to coding theory, arXiv: 1410.7184.

[Tr] H. M. Trachtenberg, On the correlation functions of maximal linear recurring sequences, Ph. D. dissertation, Univ. Southern California, Los Angles, CA, USA, 1970.

[VE] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inf. Theory, vol. 58, no. 7, pp. 4862-4869, Jul. 2012.

[WTQYX] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes and elliptic curves, IEEE Trans. Inf. Theory, vol. 58, no. 12, pp. 7253C7259, Dec. 2012.

[XI12] M. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl., vol. 18, no. 5, pp. 933-945, 2012.

[XI] M. Xiong, The weight distributions of a class of cyclic codes II, Design Codes Cryptography, to be published.

[YXDL] J. Yang, M. Xiong, C. Ding and J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory, vol. 59, no. 9, pp. 5985-5993, 2013.

[YCD] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 712-717, Feb. 2006.

[ZHJYC] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl., vol. 16, no. 1, pp. 56-73, 2010.

[ZWHZ] D. Zheng, X. Wang, L. Hu, X. Zeng, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl. 16 (5): 933-945, 2012.

[ZDLZ] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, IEEE Trans. Inf. Theory 59 (10): 6674-6682, 2013.